# INTERNAL AUDIT REPORT

# APPLICATION DATA BACKUP

*Fairfax County Internal Audit Office*

# FAIRFAX COUNTY, VIRGINIA
# INTERNAL AUDIT OFFICE
# MEMORANDUM

**TO:** Anthony H. Griffin
County Executive

**DATE:** March 30, 2000

**FROM:** Ronald A. Coen, Director
Internal Audit Office

**SUBJECT:** Report on the ***"Application Data Backup"***

This is a report on the ***"Application Data Backup."*** It was performed FY 2000 Annual Audit Plan.

The findings and recommendations of this audit were discussed with the Department of Information Technology. We have reached agreement on all of the recommendations and I will follow up periodically until implementation is complete. Their responses are incorporated into the report and the full response is attached at the end of the report. After your review and approval, we will release the report to the Board of Supervisors.

RAC:df

# TABLE OF CONTENTS

# Introduction

DIT maintains over 56,000 mainframe tape volumes to provide all County application systems with data backup for recovery capability as well as daily processing use. Approximately 3,000 tapes are located at the offsite tape storage location at the Massey Building. There are approximately 55,000 older IBM Magstar 3480 tapes and approximately 1,000 newer IBM Magstar 3590 tapes. A migration between the two types is currently in progress to achieve efficiency in disk space and reduce the physical tape storage area.

The effective management of data takes into consideration data backups, offsite storage, data retention and disposition. Control over application data ensures that data remains complete, accurate, and available during its input, update, and storage to satisfy business requirements. Key issues that pose challenges and concerns to IS management, senior management, and functional user management are:

- Complete backup of data for critical systems at off-site and on-site facilities

- Proper physical access controls (e.g. security system), and environmental controls (e.g. temperature and humidity controls)

- Coordination with contingency planning

- Awareness and communication between DIT and key system sponsors of data backup requirements

Losing the capability to retrieve and process information maintained electronically can significantly affect an organization's ability to accomplish its mission. An organization should have procedures in place to protect information resources and minimize the risk of loss and procedures to periodically review data backup provisions. These procedures should consider the activities performed at general IT support facilities, such as the data processing center and the offsite storage location, as well as the activities performed by users and custodians of specific applications. Data backup plans should be tested and reviewed periodically to determine that they will work as intended.

Senior management commitment is important to ensure that adequate resources are devoted to data backup planning and related testing. Loss of application data can result in:

- Inability to continue business functions or operations
- Loss of revenue and cash flow
- Inability to deliver products or services to customers
- Increased costs

# Purpose and Scope

This audit was performed as part of our FY 2000 long-range Audit Plan because application data backup is critical for continued County operations that use mainframe applications. Our audit objective was to assess data backups with regards to operational, archival, and disaster recovery requirements. We reviewed production backup for a sample of six mainframe application systems (FAMIS, PRISM, ADCIS, ASSIST, REABS, and PMIS/PMS). Steps have been taken to review offsite backup provisions, system sponsor knowledge and agreement, sufficiency of individual application backups, and protective/preventive measures. We did not include an overall audit of the data center operations at the Government Center.

The benefits of this audit include stronger controls, improved performance, and a report card to management on the adequacy of data backup. This audit examined application data backups and did not include review of software libraries and corresponding backups. We focused on the guidelines and procedures from the Library of Virginia (LVA) that regulates the creation, preservation, storage, filing, management and disposition of all records, including electronic records. We also referenced standards from the National Institute of Standards and Technology (NIST) including the National Bureau of Standards (NBS) Special Publication 500-101 about “Care and Handling of Computer Magnetic Storage Media”. This audit was performed in accordance with the generally accepted government auditing standards.

# Executive Summary

In our opinion, the County's mainframe application data backups meet the operational and disaster recovery needs of the organization based on our sample of mainframe application systems. The off-site backup standards were updated in August 1999 and have been approved by the CIO. DIT is actively working with the sponsoring departments to educate and update the system sponsors as to the content of the data backup and the rotation schedule. In order to attain the full benefit of the data backup plan, it is important that the system sponsors are knowledgeable and agree with the backup provisions. DIT continues to take positive steps towards improving the data backup process in the following areas:

- The appropriate offsite backup documentation was completed between DIT and the system sponsor departments.

- The data center staff conducts a monthly tape inventory of the on-site and off-site tapes. The staff conducts one third of the total inventory each month. Internal Audit conducted a physical count of a sample of tapes at the off-site facility and found no exceptions.

We identified additional improvements needed to safeguard and maintain the application data backup tapes. In the order of their importance, they are:

- The physical access controls at the off-site (Massey building) and the on-site (Government Center) are not adequate. Too many non-data center staff has access to the off-site and on-site facilities. DIT management needs to implement a much more restrictive access to these facilities.

- The fire suppression systems at the off-site and the on-site facilities pose a risk to tape backups due to the open area storage of tapes. The sprinkler systems installed at both facilities are wet pipe systems. DIT should seriously consider having redundant data backup of critical systems at both the off-site and on-site facilities.

- DIT needs documented standards/procedures for on-site and archival backups similar to the extent and level of detail as the documented standards for off-site backups.

- The system sponsors do not consistently specify the retention requirements for their backups. DIT needs to coordinate with the system sponsors to identify their data retention periods.

Recommendations to the Department of Information Technology include improving physical access and environmental controls at the off-site and on-site facilities, developing new standards for on-site and archival backups, procedures for disposition of tapes, and coordinating with the departments to identify their data retention periods.

# Comments and Recommendations

## 1. Physical access controls at the off-site (Massey building) and onsite (Government Data Center) facilities are not adequate.

There are unknown numbers of people other than the data center staff who have access to the cipher lock combination at the off-site location. There are unacceptable numbers of people who have access to the data center through multiple doors using a pass card reader or a key. On-site physical security for the tape library is significantly weakened because there is no separate and controlled tape storage area.

There are approximately 275 personnel who have access through three of the four doors to the data center where the on-site tapes are kept. We consider this number of people having access to the data center to be excessive. In our review of the 275 personnel, we found non-DIT directors, DIT educators, DIT management analysts, plumbers, carpenters, cleaning custodians, etc. who do not typically perform job related duties in the data center. Prior attempts were made by the Data Center Manager to limit the number of people accessing the data center. DIT maintains a manual log for visitors to the data center in the Production Controls area. There are two other card reader and key doors to the data center. There is also a cipher combination lock for a double door that only the data center staff has access to. It is not known when the last time the cipher combination was changed.

A maintenance worker and potentially other personnel have access to the tape storage room via a cipher combination lock at the Massey building off-site storage. During a tour of the facility with a Tape Librarian, Internal Audit observed the door propped open. Security guards stationed next to the tape room were not knowledgeable about why and how long the door was left open. It is our understanding that maintenance staffs have the combination to the off-site door to access the tape room.

Physical access controls are needed to reduce physical exposures to the backup tapes in the off-site and on-site facilities. The cipher combination locks at both facilities should be changed at least on a quarterly basis. The pass card reader access and key holders should be limited to personnel who have a business need to be in the data center. All other staff including the security guards, maintenance crew, and the cleaning custodians should be escorted at both facilities. The exposed backup tapes at the off-site and on-site facilities may be lost or removed without anyone's knowledge. In case of an interruption, the tapes may not be available to recover the data needed to resume business. There is no formal process to evaluate the physical access controls to the off-site and on-site facilities between DIT and FMD departments. The maintenance and potentially the cleaning custodian know the combination to the off-site facility; therefore, it undermines the presence of the Security Guards and the Police Officers located in the same building.

### Recommendation

We recommend that DIT take steps to substantially reduce the number of personnel who may access the data center and the off-site facility as soon as possible. At a minimum, the access to the doors leading to the data center should be limited to only the personnel who need to work in the data center. The two doors near the server room should be modified to operate as exit and not entrance doors. The fire marshall advised against eliminating these two doors entirely. These doors are used mostly as a pass through and exits. Non-data center staff such as the security guards, cleaning custodians, maintenance crew, and other County administrative staff should be required to sign in on a log kept near a door in the Production Controls area and be escorted during their visit. The Data Center manager should change the cipher combination lock at least quarterly at the on-site facility.

We recommend DIT change the cipher combination lock quarterly at the off-site facility to prevent non-data center staff from accessing the tape room. Arrangements should be made with the security guards located on the same floor to log their routine check of the tape room. DIT can work with the FMD to coordinate the cleaning of the tape room with the daily scheduled tape rotation.

### Additional Security Considerations

- DIT should also consider a more restricted access to tape library contents through the installation of a separate tape library room in the data center. The relative need for this additional protection will depend upon the level of access restriction achieved for the data center. If this alternative is chosen, the tape library room should be located near the data center staff who administers the tapes for backup and retrieval. A separate tape library reduces the risk that unauthorized personnel are able to access the tapes in the library.

- In addition, management may wish to consider installing cameras at key entrances and in the tape area in order to have regular surveillance of the data center and assist the limited number of data center staff, who will be required to escort all visitors. This will support continuous monitoring of the data center. A door alarm system would be helpful to monitor people entering and leaving the facility and any reference made such as signs and labels on the doors, walls, and directories to identify the data center location should be removed.

### Department Response

DIT concurs with the recommendation. Cipher locks at the Government Center computer center and at the Massey tape storage room have been changed. DIT will determine the feasibility of including the checking of the tape room by security guards during their routine duties. DIT is working with FMD to modify the security system to support the limited access to the Government Center computer center. DIT has requested funds to engage a consultant to perform a detailed review of the computer room physical site and related security. Additionally, DIT will investigate the feasibility of commercial offsite tape storage, especially for critical applications.

### 2. The fire suppression systems at the off-site and the on-site facilities pose a risk to tape backups due to the open area storage of tapes.

Water sprinkler (wet pipe) systems are in place at both locations. In the on-site facility, the old tapes (IMB Magstar 3480) are also mounted on open racks, and the new tapes (IBM Magstar 3590) are encased in a vented metal frame (IBM Magstar 3484). The exposed old tapes are not protected from the water sprinkler system (wet pipe). IBM representatives stated the encased new tapes are not protected from water discharge. Backup tapes should be protected from exposure to excessive heat, humidity and potential water damage to the extent possible. In the recent past, most major data centers including the County, used Halon gas as the major fire suppression system. In cases where tapes are exposed to the risk of water damage, additional measures should be employed to reduce potential loss of data. We found no authoritative source that would support magnetic tape data integrity subsequent to water exposure. There is a risk that County data files could be lost in the event of a sprinkler system discharge. A sprinkler discharge is more likely than a major data center fire. Departments will not be able to rely on the backup tapes to restore data and resume their business.

The offsite is used as a storage facility to keep the backup tapes of two generations for disaster recovery purposes. With exception to the fire alarm, no planning was made to safeguard the backup tapes from the water sprinkler (wet pipe). Similarly, no further planning was made to protect the backup tapes at the on-site facility. The old and the new tapes in the data center are subject to damage in case of a water leak or when the water sprinkler is activated.

### Recommendation

We recommend DIT maintain tape backup redundancy at both the off-site and on-site facilities. At a minimum, management should have tape backup redundancy for critical application systems. DIT should inform and come to an agreement with the sponsoring departments as to whether their systems are determined as critical or non-critical. This recommendation is the least costly option.

DIT should consider other alternatives in the long term. These alternatives are costly, but do provide additional protection for County data backups.

- We believe the most effective alternative would be the installation of a tape vault. A tape vault eliminates exposure to water sprinklers and potential damage from smoke or heat.

- Another alternative is for DIT to consider converting wet pipes to inert gases (e.g. halocarbon agents) at both tape storage facilities. Inert gases are less effective than Halon that was banned in January 1994. Unlike Halon, inert gases have no negative impact on the environment. They also produce very little acid gas products during fire suppression, decreasing possible damage to sensitive electronic equipment. However, safety is a concern since inert gases rely on diluting oxygen in the room to suppress a fire.

- DIT should also consider improving the existing fire suppression systems installed and protection for tapes at the off-site and on-site facilities. The water sprinkler systems installed at both facilities could be converted from wet pipes to dry pipes. This will only provide marginal improvement to our existing wet pipe system. The water is discharged only when a heat or smoke sensor is activated. A water sprinkler system is more effective than Halon (fire suppressor) at putting out deep-seated fires. However, accidental release of water due to a damaged sprinkler head is still a potential occurrence that can cause serious damage to the computer equipment.

### Department Response

DIT concurs with the recommendation. Evaluation of existing and improved environmental controls and supporting equipment for the fire suppression systems to protect the tape backups will be part of the consultant’s review that will incorporate the multiple suggestions made in the audit report.

### 3. Tape related procedural and guideline documentation is not available for on-site and archival backups, disposition of tapes, and methodology for scheduled tape read/write to address retention periods exceeding the life span of the tapes.

DIT has updated the 1991 off-site backup standard in August 1999. The CIO has recently signed and approved the document. As stated in the off-site backup standards, the documentation does not cover on-site and archival backups. There is no clear distinction between what are on-site versus off-site tapes. For example, the archival tapes are available at both the on-site and off-site facilities based on the tape inventory list reviewed.

There is no documented process for disposing the tapes that are no longer in use. In the past, a contractor was hired to dispose of the tapes. The Data Center staff degaussed the tapes before they were turned over to the contractors. Some older tapes are still kept at the data center pending further action. There is no methodology for scheduling tape read and write to another media to retain the data longer than the 10 year warranty on the IBM Magstar tapes. However, the data center is currently in the process of writing (copying) the old tapes to the new tapes that have more storage capacity. Approximately 4% or 2,200 of the County’s tapes have been retained for periods exceeding 10 years.

Documented procedures are necessary that includes on-site and archival backups. An on-site standard will address what datasets, how many generations, whether tapes should be redundant as off-site, and software and related documentation are to be kept at the on-site as compared to the off-site facility. An archival standard ensures those archival meet legal and business requirements by addressing the appropriate data retention period and where the archived data will be kept. Appropriate disposition of tapes will ensure against a breach in information for medical, criminal, and other sensitive data. A methodology should be in place to read and write tapes marked as permanent and retention periods exceeding the warranty period of the tapes. The absence of guidelines will cause inconsistencies as to where certain backup contents (data, program, libraries, etc.) are to be kept and how these backups (on-site and archival) are to be administered effectively for immediate retrieval, timely disposition of tapes, and tape migration.

DIT has focused on the importance of developing a standard for off-site backup. They are planning to include standards for on-site and archival backups in the near future. The infrequency of the need to dispose of the tapes and copying the tapes to another media precluded DIT staff from documenting these processes.

### Recommendation

We recommend DIT develop a standard for on-site and archival backups similar to the extent and level of detail as the standard for off-site backup. At a minimum, the standards should include periodic inventory of tapes, whether tapes should be redundant at the off-site facility and software and related documentation requirements are sufficient to backup and recover tapes.

We recommend DIT develop a documented procedure to properly handle the disposition of tapes, as they affect both the security and confidentiality of the data. For example, the tapes may have to be degaussed more than once, especially for some of the application systems from Human Resources

(PRISM), Public Safety (PMIS/PMS), and Human Services (ASSIST) that may have personnel, criminal, and client medical records considered as confidential. The Library of Virginia has developed a guide for the disposition of electronic media that could be used to develop the in-house procedure.

We also recommend DIT develop a methodology to copy long-term archived data after a specified number of years. Some of the County's archived data is retained for as long as 20 years. Copies should be made as necessary or when the read error rate is determined to be unacceptable. As a reference, the State Library Board issues regulation governing the retention and disposition of state and local government records. The guidelines for Managing Electronic Records (issued 1994) and a policy for the Retention, Maintenance & Disposition of Digitized Visual Public Records (Rev: 1/96) explains the criteria for managing electronic records, the frequency of reading stored data, and writing to a new media. It states, in part, that the maintenance of tapes includes:

- Testing the tapes no more than 6 months prior to using them to store electronic records

- Storage and test areas for tapes shall be kept at a constant temperature (62 F to 68 F) and constant relative humidity (35% to 45%)

- A statistical sampling of tapes to be read annually to identify any loss of and to discover and correct the cause of the data loss

- Data tapes shall be copied before the tapes are 10 years old

### Department Response

DIT concurs with the recommendation. DIT will develop a standards document that will support the on-site backup and archival tape requirements, disposal of all damaged and retired tapes, and define the processes necessary to ensure that data always resides on tapes that are within their manufacturer's recommended life expectancy.

## 4. System sponsors do not consistently specify the retention requirements for their backups.

Data retention requirements are not specified by most of the departments on the "Offsite Tape Backup Specifications" forms kept at the Data Center. In the absence of the data retention information, DIT flags the expiration date as "Catalog." A catalog designation requires the tape system to retain the data until a specified number of generations are backed up and the older generation rolls off for deletion.

Departments must specify, in terms of a date (Julian date), a cycle or a number of generations the retention period on the "Offsite Tape Backup Specifications" form to DIT. This is specified in the off-site backup standards documentation. Departments may not be able to respond timely to requests for data from their customers, regulatory departments, vendors, and other business parties without appropriate retention of tapes. In addition, without proper data retention, default retention time frame may be applied that are not related to system sponsor needs. Departments may not be fully aware of their data retention requirements. Some are under the false impression that their data will be kept for an indefinite period of time.

### Recommendation

We recommend DIT work with the departments to identify their data retention requirements. The departments, as owners of the data, need to specify how long archival data must be kept to meet their business needs by contacting the appropriate local, state and/or federal archives, federal and state agencies (e.g. grantors and IRS). This may be specified in terms of a number of generations, specific dates or permanent retention. Departments may need to work with the County Attorney's Office to determine the statute of limitation for their unique set of data, such as taxes, deeds, etc. The County's Document Services Division, which is now under the Department of Telecommunications & Consumer Services, has a manual developed by the Library of Virginia governing the retention and disposition of state and local government records. This information is available on the Internet address: http://www.lva.lib.va.us.

### Department Response

DIT concurs with the recommendation. DIT staff will meet with representatives of sponsoring departments to determine appropriate off-site and on-site backup retention requirements for each department and record the results in the "Computer System Abstract" for each system.

### 5. Temperature and humidity controls at the off-site backup facility (Massey Building) and at the on-site facility (Government Center) are not monitored through the appropriate equipment/devices that are regulated.

An air conditioning system is left on at the off-site facility around the clock to control the temperature of the tapes mounted on multiple racks. According to IBM specifications, the temperature for the tapes should be between 60 and 90 degree Fahrenheit. The humidity reading should be between 20 and 80% relative humidity. DIT meets the tape temperature and humidity requirements. Currently, only the on-site facility has an air conditioning unit with an alarm system that would be activated when the temperature in the area exceeds a certain tolerance level.

Environmental controls such as smoke, heat, and fire detection equipment and fire extinguishers are commonly found in data centers. Good housekeeping controls are part of the environmental controls. Heat and humidity control devices are also normally used to regulate the environment.
The environmental controls relative to tape cartridges should be the same for off-site and on-site facilities. The long-term reliability of magnetic tape storage is degraded by improper environmental controls for temperature and humidity. Departments that depend upon long term availability of records may not be able to rely on this medium. No planning was made to introduce environmental checks to control temperature and humidity for the magnetic tapes based on vendor specifications or industry standards.

### Recommendation

We recommend DIT periodically take the temperature and humidity reading at the off-site and on-site facilities. If there is a variation from the environmental specifications mentioned earlier, DIT should consider having FMD install the appropriate environmental controls at the off-site and on-site facilities to regulate the temperature and the humidity for the backup tapes.

### Department Response

DIT concurs with the recommendation. Evaluation of existing and improved environmental controls and supporting equipment for monitoring temperature and humidity controls at the Massey and at the Government Center will be part of the consultant's review.